All Sectors Bulletin

OS Assessment - Colonial Pipeline Hack/Implications

Overview

On Saturday May 7th the Colonial Pipeline Company took some of their systems offline after learning it was the victim of a ransomware cyber-attack. The attack and subsequent shutdown resulted in a halt in operations of their 5,500-mile long pipeline spanning 11 states from New Jersey to Texas and responsible for around 45% of the East Coast's diesel, petrol, and jet fuel. Colonial Pipeline immediately began working with law enforcement and several federal agencies with the Department of Energy leading the government's response. According to open source sources, the ransomware cyber-attack hit the IT portion of the company's network and not to operational technology which controls pipeline functionality.

Parts of the pipeline were reactivated earlier in the week and by 5:00pm ET on Wednesday May 12th, Colonial Pipeline had initiated a restart of the pipeline operation. It will take several more days for product delivery to the full supply chain returns to normal, with most markets expected to receive product by Thursday afternoon.

Shortages

Significant fuel shortages have been reported in all the states serviced by the pipeline with authorities quickly advising people to avoid panic buying and only get the gas needed through the week/weekend. Gas prices swiftly increased as some gas stations ran out of fuel while others limited purchases, commonly capping at 10 gallons or $30 dollars per vehicle. The fuel shortage also impacted air travel with American Airlines adding temporary refueling stops to long-haul flights out of North Carolina and Southwest Airlines flying planes with extra fuel into airports in the impacted area including Tennessee.

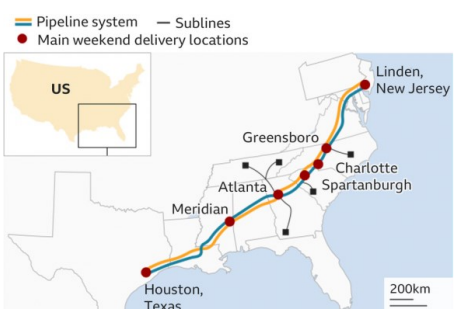
In response to the shortages and after reports of significant price increases and lines at the pump, Virginia Governor Ralph Northam and Florida Governor Ron DeSantis declared states of emergency. The federal government responded with several measures including relaxing rules on the transportation of fuel by road to minimize supply disruption.

Most officials now believe that by the weekend most people will not have issues finding and buying gas.

Cyber-attack

The cyber-criminal group DarkSide claimed responsibility for the attack, releasing a statement reading "our goal is to make money and not creating problems for society" and clarified that they are apolitical and unaffiliated with any government. The group, which offers ransomware to affiliates for a percentage of earning in any successful attacks, stated they weren't aware that an affiliate was targeting Colonial Pipeline and added that "from today, we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

The attackers stole nearly 100 gigabytes of data and threatened to leak the information on the internet if payment wasn't received. Earlier in the week the FBI officially confirmed DarkSide as responsible.



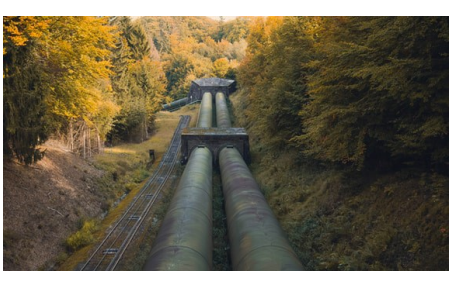
-Resources-

Best Practices for Organizations

- Ensure that all systems and antivirus software are updated. This reduces vulnerability and increases the chances of early detection of malicious activity.
- Minimize internet-facing remote access solutions. When possible, enforce VPN usage for all privileged remote connections.
- Separate Industrial Control Systems from service and business networks. Network segmentation can severely disrupt malicious actors attempting to move laterally throughout the network.
- Encourage organizational IT and cyber security teams to perform audits of security compliance throughout networks within the organization.
- Maintain a series of backups for all critical systems on your network. In an ideal configuration there should be an online and offline backup. In the event an incident occurs and the validity of the online backup cannot be confirmed, an offline backup can rapidly accelerate the recovery process.
- Organizations should work to increase network visibility and remain aware of potential data exfiltration.

Info on Darkside

- Darkside is the group of malicious actors associated with the shutdown of the Colonial Pipeline on May 7th, 2021.
- Darkside presents as a "Robinhood group". They have publicly stated their intentions to donate proceeds from their operations to charitable organizations.
- At this time it is believed that Darkside will not target civilian non-profits and hospitals.
- Darkside is a Ransomware-as-a-Service (RaaS) model in which customers can pay for an attack to be conducted against a specific organization.



Pipeline Cybersecurity Initiative

CISA, through the National Risk Management Center (NRMC), is managing the Pipeline Cybersecurity Initiative (PCI), by leveraging expertise from government and private partners to identify and address cybersecurity risks to enhance the security and resiliency of the Nation's pipeline infrastructure.

View Resource →

Infrastructure Security

CISA works with businesses, communities, and government at every level to help make the nation's critical infrastructure more resilient to cyber and physical threats. Everyone has a role securing the Nation's critical infrastructure.

View Resource →

Sources:

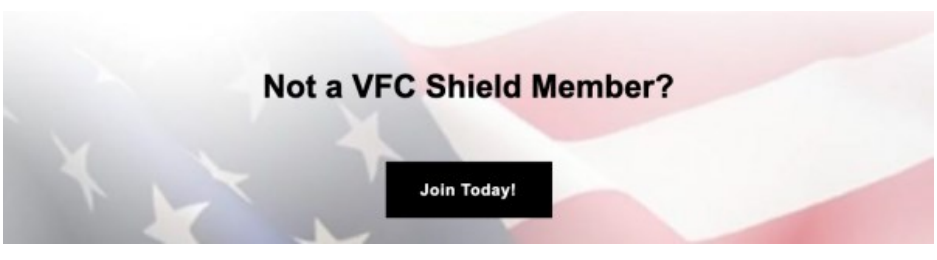
- New York Times - Pipeline Hack Points to Growing Cybersecurity Risk for Energy System
- CNN - Gasoline demand spikes in several states after pipeline hack
- Colonial Pipeline – Press Releases
- ARS TECHNICA – Colonial Pipeline Resumes Operations After Ransomware Prompted Closure
- BBC News - US fuel pipeline hackers 'didn't mean to create problems

View Virginia Fusion Center Homepage

Click Here

Observe Suspicious Activity?

Report Online



"Awareness Through Information Sharing"

This assessment is the result of collaboration and cooperation with the Hanover County Sheriff's Department.

VFC Shield

"Awareness Through Information Sharing"

Need Help with this Email?

View in a browser

Useful Links

- VFC Fusion Site
- Shield Homepage
- All Products
- Report SAR
- Email Coordinator